DATE: JUNE 1, 2019

MEMORANDUM FOR THE RECORD

FROM: JOSEPH F. SCHATZ III, DEPUTY DIRECTOR OF WHITE HOUSE INFORMATION TECHNOLOGY

SUBJECT: SECURITY FIRST – OCISO AND OA OCIO MUST REMAIN INDEPENDENT OFFICES

(U//FOUO) Within the Executive Office of the President (EOP), the Office of the Chief Information Security Officer (OCISO) was established in 2015 as a response to a major security incident, and is responsible for the information security of the Presidential Information Technology Community (PITC) networks. According to a US Intelligence Community (USIC) assessment from 2015, prior to the establishment of the Director of White House Information Technology (D/WHIT) and CISO positions, the PITC was "operating ineffectively under disparate authorities" [and] defined by a "lack of clear governance roles, responsibilities, and relationships pertaining to requirements, security assessment, and authorization, acquisition, and technology investments."[1] Furthermore, the USIC analysis states that "it is imperative that [the D/WHIT and CISO] roles and authorities are quickly established and codified."[2] The nation's most critical intelligence, military, and diplomatic information passes through the PITC network,[3] and the security of the network therefore has global implications. It is the responsibility of the OCISO to "assesses the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets" of the President.[4]

(U//FOUO) Since 2015, the OCISO has significantly matured the information security posture of the EOP and built a robust cyber security program, insider threat program, user awareness program, and digital forensics unit from the ground up. The OCISO has established a "security-first" culture, with multiple teams working to protect the PITC network and the devices and personnel of all EOP components – including the White House Office, National Security Council, US Trade Representative, Office of Management and Budget, and the Office of Administration – no matter where in the world EOP staff are traveling. Under the direction of the OCISO, the White House Threat Intelligence, White House Computer Network Defense, Data Loss Prevention, and Information Assurance teams work to protect the PITC network from sophisticated nation-state cyber intrusion sets, insider threats, and the compromise of sensitive information. These teams support all EOP components by monitoring nation-state intrusion sets and implementing defensive countermeasures on the network; providing 24/7 network and email monitoring; proactively identifying and investigating leaks of sensitive information, such as the President's movements and schedule, which have a direct impact on his physical security; authoring technical threat memos and guidance to support POTUS, VPOTUS, APNSA, and other VIP delegations traveling outside the contiguous United States (OCONUS); briefing senior delegations and PITC partners on the technical threat environment in foreign countries; traveling OCONUS to high-threat locations to provide on-site cyber intelligence and network defense support; authorizing White House Information Technology-issued electronic devices on foreign travel; and providing cyber awareness and onboarding briefings, as well as personalized Cyber Hygiene Reviews, for senior

staff. None of these capabilities existed at the White House prior to their establishment by the OCISO.

(U//FOUO) This maturation of the EOP's OCISO responsibilities parallels industry and government standards for risk management, compliance, and enforcement. Industry best-practices elevate enterprise security to an executive-level issue and business priority, with the OCISO reporting directly to organizational leadership, rather than through an OCIO.[567] At one of our USIC partner agencies, the CIO and CISO positions are separated for precisely this reason, with different reporting chains and directorates.[8] Due to the potential for conflicts of interest between organizational OCISO and OCIO positions, the Sarbanes-Oxley Act (SOX) mandates OCISO independence for the financial sector under its "separation of duty" requirement. Primary reasons for separating OCISO and OCIO positions within organizations include: operational conflicts between keeping systems running (OCIO) and lowering information technology risk (OCISO); the need for the OCISO to make risk-based decisions at an operational level with physical security, human resources, legal counsel, and other departments; the need for the OCISO to identify malicious insiders, including those involved in IT and under the OCIO's purview; the need to "solve problems without technology," for example via educational and awareness programs; and legal regulations surrounding conflict of interest which mandate security integrity, such as SOX.[9] According to a 2017 survey from the Ponemon Institute, which conducts independent research on data protection, information technology, and the threat landscape, 65% of CISOs report directly to senior executives, and 68% of organizations now give CISOs the final say in all IT-security spending. Furthermore, 69% of respondents consider the appointment of an executive-level security leader with enterprise-wide responsibility as an organization's most important governance practice."[10] This elevation of the OCISO to an executive-level position is a best-practice recommended by leading security researchers since at least 1997.[11]

(U//FOUO) As the White House has matured its "security-first" processes and capabilities for the EOP and the PITC networks, the OCISO has been formalized as an independent entity – responsible for the management of information security, assessing the risk and magnitude of harm resulting from unauthorized access, and independently verifying the security of products and services, regardless of internal pressures. Importantly, the OCISO is responsible for providing this security function for all EOP components and PITC partners – including the White House Military Office, the White House Communications Agency, the NSC, USTR, and OA. This OCISO oversight of all EOP components – and direct access to EOP executive leadership – demonstrates the White House's commitment for security, and is critical for the protection of the PITC network from both highly sophisticated nation-state actors and from insider threats. As such, it is imperative that the OCISO remain able to assess risk to the EOP in a holistic manner which is independent of the OCIO and other internal pressures, which can incentivize delivering products quickly to meet customer needs and shortcutting security considerations. Placing this office under the Office of Administration (OA) Office of the Chief Information Officer (OA OCIO) would create an operational conflict and a level of risk for the EOP that is diametrically opposed to my responsibility to protect this nation's most critical information, networks, and personnel. Moreover, it is my professional judgment that this measure would result in an immediate and significant negative impact on the security of the PITC network, as well as the protection of White House assets and personnel. Finally, the White House networks have not been breached under my watch. We are utilizing industry and government recommendations to have OCISO separated from

OCIO. If EOP leadership makes the decision to move OCISO back under OCIO, the White House would divert from the best-in-breed corporate and USIC recommendations to have the OCISO remain independent. Such a decision would revert the EOP back to a pre-2015 organizational structure, significantly inhibit the CISO's ability to successfully mitigate risk across the EOP enterprise, and move the White House and the President toward a path whereby an adversary could successfully attack and compromise the network.

---

[1] (U//FOUO) White House Classified Information Technology Systems Assessment, Version 1.5 Final; Page 6. Cited portion is U//FOUO.

[2] (U//FOUO) White House Classified Information Technology Systems Assessment, Version 1.5 Final; Page 6. Cited portion is U//FOUO.

[3] (U//FOUO) White House Classified Information Technology Systems Assessment, Version 1.5 Final.

[4] (U//FOUO) USIC Partner; Chief Information Security Officer (CISO)/ Senior Agency Information Security Officer (SAISO); Cited portion is UNCLASSIFIED.

[5] (U) ISACA; "State of Cybersecurity, Implications for 2016: An ISACA and RSA Conference Survey. Page 5. Accessed 30 May 2019 at http://[illegible]_eng_0316.pdf.